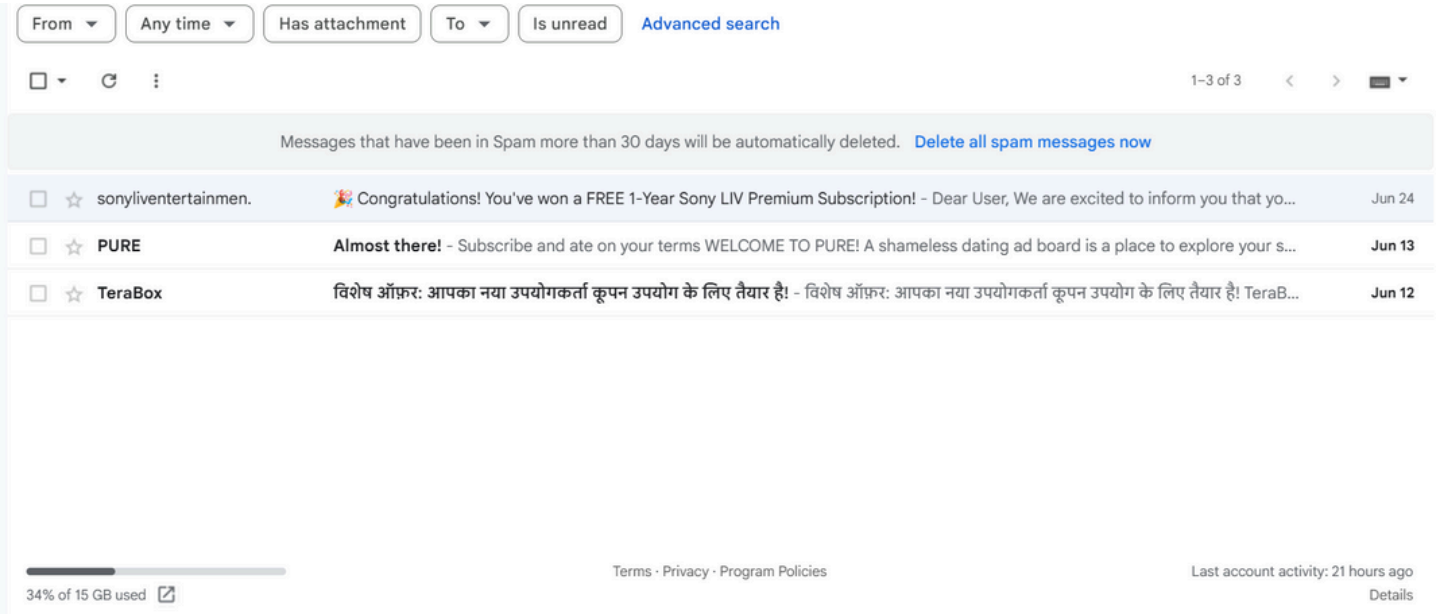
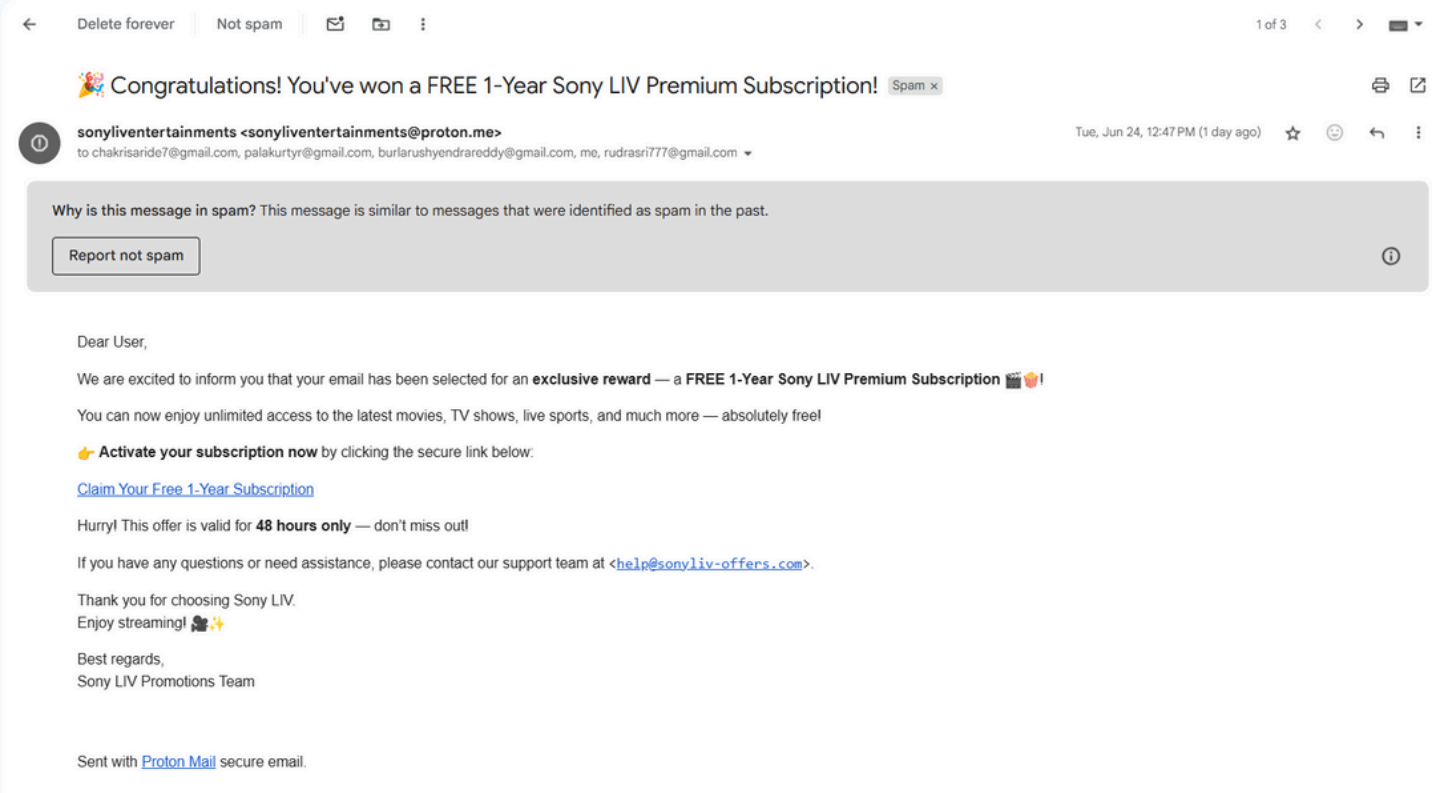
ELEVATE LABS CYBERSECURITY INTERNSHIP TASK-2

1) i created a spam email named sonyliventertainments made it look like a spam mail stating that user got a free subscription of sonyliv for a year with a link that’s leading to some other website





2)

Original Message

Message ID	<cJKSg3j4aHTCVXNWuthdkfSI1Wo43vmH21M6lEQ5xhn2peu_9VcwvQeMVhq-jGHy7k10uNVz6S0TfBugi4bfki_YDIOcHKImPxkNINUOWWw=@proton.me>
Created at:	Tue, Jun 24, 2025 at 12:47 PM (Delivered after 6 seconds)
From:	sonyliventertainments <sonyliventertainments@proton.me>
To:	"chakrisaride7@gmail.com" <chakrisaride7@gmail.com>, "palakurtyr@gmail.com" <palakurtyr@gmail.com>, "burlarushyendrareddy@gmail.com" <burlarushyendrareddy@gmail.com>, "siddhuvajjula@gmail.com" <siddhuvajjula@gmail.com>, "rudrasri777@gmail.com" <rudrasri777@gmail.com>
Subject:	🎉 Congratulations! You've won a FREE 1-Year Sony LIV Premium Subscription!
SPF:	PASS with IP 185.70.43.19 Learn more
DKIM:	'PASS' with domain proton.me Learn more
DMARC:	'PASS' Learn more

Download Original

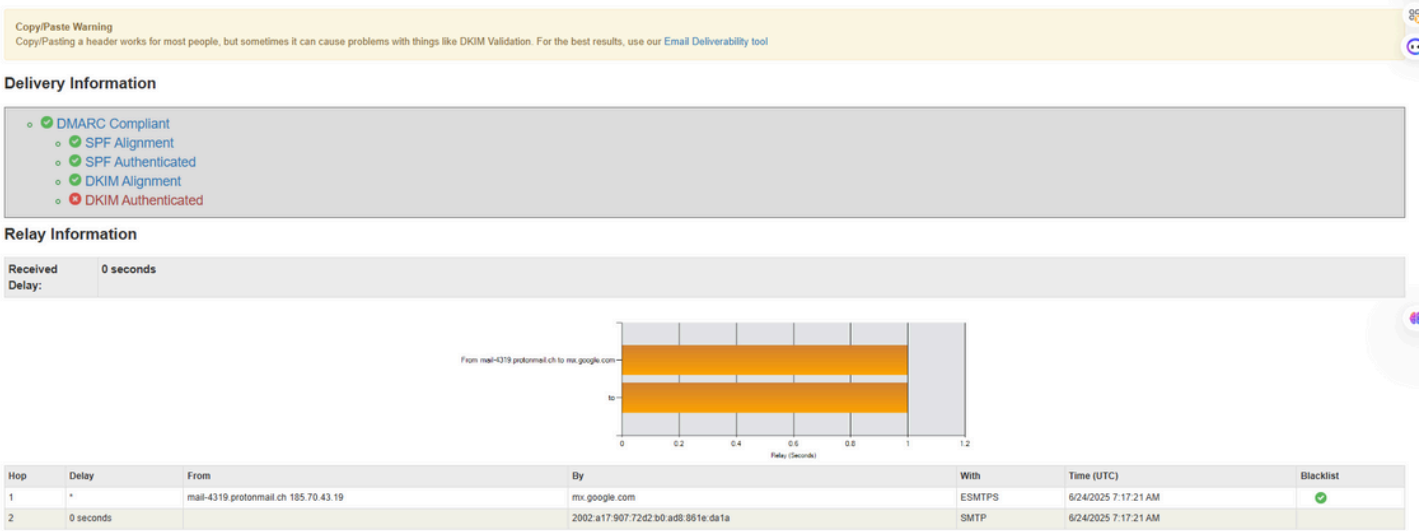
Copy to clipboard

we used tool email analyser and pasted email header there to analyse

Although the email passed SPF, DKIM, and DMARC verification, it uses a **ProtonMail** domain rather than an official **Sony** domain, which is a strong indicator that it is not legitimate. The display name, “sonyliventertainments,” can be easily spoofed and doesn’t confirm the sender’s true identity.

While the successful SPF, DKIM, and DMARC checks show that the message was authorized to be sent from **ProtonMail’s servers**, they do not confirm any affiliation with **Sony**. The absence of official Sony branding, a verified Sony domain, or trusted links further raises suspicion.

3)



- **Result:** DMARC is configured (v=DMARC1), set to **quarantine**.
- Policy (p=quarantine) means emails failing DMARC checks will be placed in spam/quarantine.
- DMARC settings:
  - fo=1: Enables DMARC Failure Reports.
  - aspf=s: SPF alignment is strict.
  - adkim=s: DKIM alignment is strict.

Implication: DMARC is properly configured for the proton.me domain and will help prevent unauthorized senders from successfully sending spoofed emails.

SPF Alignment and Authentication

- SPF record (v=spf1 include:_spf.protonmail.ch ~all) passed.
- The sender's IP (185.70.43.19) is listed as a valid IP for proton.me.
- Result: SPF is aligned and the email is **SPF Authenticated**.

Implication: This confirms that the sending server is authorized to send emails on behalf of proton.me, making it highly unlikely this email is spoofed.

The email was relayed from:

- mail-4319.protonmail.ch (185.70.43.19) ➔ mx.google.com

Delivery time between the servers was almost instantaneous (0 seconds), indicating low network delay and suggesting a legitimate email path.

4)

Dear User,

We are excited to inform you that your email has been selected for an **exclusive reward** — a **FREE 1-Year Sony LIV Premium Subscription** 🎬🍿!

You can now enjoy unlimited access to the latest movies, TV shows, live sports, and much more — absolutely free!

👉 **Activate your subscription now** by clicking the secure link below:

Claim Your Free 1-Year Subscription

Hurry! This offer is valid for **48 hours only** — don't miss out!

If you have any questions or need assistance, please contact our support team at <help@sonyliv-offers.com>.

Thank you for choosing Sony LIV.
Enjoy streaming! 🎥✨

Best regards,
Sony LIV Promotions Team

hyperlink stating that Claim your oer which might be an unsecure website when entered and if any details are provided this may lead to leaking of the users sensitive information

5)

Claim Your Free 1-Year Subscription

Hurry! This offer is valid for **48 hours only** — don't miss out!

If you have any questions or need assistance, please contact our support team at <help@sonyliv-offers.com>.

Thank you for choosing Sony LIV.
Enjoy streaming! 🎥✨

Best regards,
Sony LIV Promotions Team

6)link we can see that we are being redirected to some random IP